**Ўзбекистон Республикасининг “Электрон рақамли имзо тўғрисида”ги Қонунининг янги таҳририни ишлаб чиқиш доирасида   
халқаро тажрибани ўрганиш бўйича тайёрланган   
ТАҲЛИЛИЙ МАЪЛУМОТЛАР**

Ўзбекистон Республикаси Президентининг “Рақамли Ўзбекистон – 2030” стратегиясини тасдиқлаш ва уни самарали амалга ошириш чора-тадбирлари тўғрисида” 2020 йил 5 октябрдаги ПФ-6079-сон Фармони қабул килинган.

Ушбу Фармон билан тасдикланган 2020-2022 йилларда “Ракамли Ўзбекистон – 2030” стратегиясини амалга ошириш буйича “йул харитаси”нинг (24-илова) 8-бандида Ўзбекистон Республикасининг “Электрон рақамли имзо тўғрисида”ги Қонунининг янги таҳририни ишлаб чиқиш топширғи юклатилган.

Мазкур топшириқ ижросини таъминлаш мақсадида Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги ҳамда манфаатдор вазирлик ва идоралар билан хамкорликда Ўзбекистон Республикасининг “Электрон рақамли имзо тўғрисида”ги Қонунининг янги таҳририни ишлаб чиқиш бўйича таҳлилий маълумот тайёрланди.

**I. Ўзбекистон Республикасининг “Электрон рақамли имзо тўғрисида”ги қонуни ижросининг жорий ҳолати.**

Электрон рақамли имзо калитларини рўйхатдан ўтказиш марказларининг рўйхатга олиш органининг вазифалари ва функцияларини бажаришда Ўзбекистон Республикасининг “Электрон рақамли имзо тўғрисида”ги Қонуни ва Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2005 йил 26 сентябрдаги 215-сонли Қарори билан тасдиқланган “Электрон рақамли имзолар калитларини рўйхатга олиш марказларини давлат рўйхатидан ўтказиш тартиби тўғрисида низом” асосида амалга оширилади.

Ўзбекистон Республикаси Президентининг 2005 йил 8 июлдаги   
ПҚ-117-сонли “Ахборот-коммуникация технологияларини янада ривожлантиришга оид қўшимча чора-тадбирлар тўғрисида”ги Қарори билан Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги электрон рақамли имзолардан фойдаланиш соҳасида махсус ваколатли орган сифатида белгиланган.

Электрон рақамли имзолардан фойдаланиш соҳасидаги махсус ваколатли органнинг асосий вазифалари ва функциялари:

* электрон рақамли имзодан фойдаланиш стандартлари, нормалари ва қоидаларини ишлаб чиқади;
* электрон рақамли имзолар калитларини рўйхатга олиш марказларини давлат рўйхатидан ўтказади;
* рўйхатга олиш марказлари ваколатли шахсларига тегишли электрон рақамли имзолар калитлари сертификатларининг ягона давлат реестрини юритади ҳамда юридик ва жисмоний шахсларнинг ундан эркин фойдалана олишини таъминлайди;
* рўйхатга олиш марказларининг ваколатли шахсларига электрон рақамли имзолар калитлари сертификатларини беради;
* юридик ва жисмоний шахсларнинг мурожаатига биноан рўйхатга олиш марказлари ваколатли шахсларининг электрон рақамли имзоси ҳақиқийлигини тасдиқлайди;
* қонун ҳужжатларига мувофиқ бошқа ваколатларни амалга оширади.

Электрон рақамли имзолар калитларини рўйхатга олиш марказларининг асосий вазифалари ва функциялари қуйидагилардир:

* электрон рақамли имзоларнинг ёпиқ ва очиқ калитларини яратади;
* электрон рақамли имзо ёпиқ калити муҳофаза қилинишини таъминлайди;
* электрон рақамли имзолар калитлари сертификатларининг реестрини юритади, унинг ўз вақтида янгиланишини ҳамда ундан юридик ва жисмоний шахсларнинг эркин фойдалана олиш имкониятини таъминлайди;
* юридик ва жисмоний шахсларга электрон рақамли имзолар калитларининг сертификатларини электрон ҳужжатлар шаклида ва қоғоз ҳужжатлар шаклида беради;
* электрон рақамли имзолар калитлари сертификатларининг амал қилишини тўхтатиб туради ва қайта тиклайди, шунингдек уларни бекор қилади;
* юридик ва жисмоний шахсларнинг мурожаатига биноан электрон рақамли имзолар калитлари сертификатларининг кўчирма нусхалари берилишини, шунингдек электрон рақамли имзолар калитларининг тўхтатиб турилган ва бекор қилинган сертификатлари тўғрисидаги маълумотлардан эркин фойдаланилишини таъминлайди;
* юридик ва жисмоний шахсларнинг мурожаатига биноан электрон ҳужжатлардаги электрон рақамли имзонинг ҳақиқийлигини тасдиқлайди;
* электрон рақамли имзоли қоғоздаги электрон ҳужжатларнинг кўчирма нусхаларини тасдиқлайди;
* электрон рақамли имзо калитининг сертификатидан бундан буён фойдаланиш имкониятига таъсир этиши мумкин бўлган ҳоллар ҳақида электрон рақамли имзо ёпиқ калитининг эгасини хабардор қилади;
* электрон рақамли имзо ёпиқ калитининг эгаларини электрон рақамли имзодан фойдаланиш қоидаларига ўқитиш имкониятини таъминлайди.

Бугунги кунга келиб, Ўзбекистон Республикасида ЭРИ калитларини рўйхатдан ўтказиш давлат органлари ҳузурида ишлайдиган 6 та Марказ томонидан амалга оширилмоқда.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Номланиши** | **Юридик шахсларга** | **Жисмоний шахсларга** | **Актив холатда** | **Жами** |
| 1 | Ўзбекистон Республикаси Давлат солиқ қўмиатси ҳузуридаги “Янги технологиялар” илмий-ахборот маркази | 1 873 802 | 4 329 411 | 3 058 587 | 6 203 213 |
| 2 | «UNICON.UZ» ДУК | 243 793 | 10 874 | 50 934 | 254 667 |
| 3 | Ўзбекистон Республикаси Молия вазирлиги ҳузуридаги Ахборот ҳисоблаш маркази | 2 669 | - | 2 665 | 2 669 |
| 4 | Ўзбекистон Республикаси Марказий банки Хавфсизлик ва ахборотни муҳофаза қилиш департаменти | - |  | 85 536 | 264 867 |
| 5 | Навоий кон-металлургия комбинати | - | 727 | 621 | 727 |
| 6 | Электрон онлайн-аукционларни ташкил этиш маркази | 5 616 | 3 533 | 99 | 9 149 |
|  | **Жами** |  | | **3 198 442** | **6 735 292** |

ЭРИ калитларини рўйхатдан ўтказиш марказлари криптографик алгоритмлардан фойдаланган ҳолда калитларни ишлаб чиқаради: O‘zDSt 1092:2009 (I-алгоритм, II-алгоритм), RSA ва ГОСТ Р 34.10-2001.

Рўйхатдан ўтиш марказлари контекстида ишлатилган ЭРИ алгоритмлари берилган қуйидаги жадвалда:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Номланиши** | **RSA** | **O‘zDST 1092:2009**  **I-алгоритм** | **O‘zDST 1092:2009**  **II-алгоритм** | **ГОСТ Р 34.10-2001** |
| 1 | Ўзбекистон Республикаси Давлат солиқ қўмиатси ҳузуридаги “Янги технологиялар” илмий-ахборот маркази | - | – | + | - |
| 2 | «UNICON.UZ» ДУК | + | + | + | + |
| 3 | Ўзбекистно Республикаси Молия вазирлиги ҳузуридаги Ахборот ҳисоблаш маркази | - | + | - | + |
| 4 | Ўзбекистон Республикаси Марказий банки Хавфсизлик ва ахборотни муҳофаза қилиш департаменти | + | - | - | - |
| 5 | Навоий кон-металлургия комбинати | + | + | - | - |
| 6 | Электрон онлайн-аукционларни ташкил этиш маркази | - | - | + | - |

*(Изоҳ: «UNICON.UZ» ДУК, Ўзбекистно Республикаси Молия вазирлиги ҳузуридаги Ахборот ҳисоблаш маркази ва Навоий кон-металлургия комбинати, Электрон онлайн-аукционларни ташкил этиш маркази учун ЭРИ калитларни генерация қилиш дастурий таъминоти - «UNICON.UZ» ДУК мутахассислари томонидан ишлаб чиқилган ва амалга оширилган).*

Электрон рақамли имзо соҳасида Ўзбекистон Республикасида қуйидаги стандартлар қабул қилинган:

1. O‘z DSt 1092:2009 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жара-ёнлари”;

2. O‘z DSt 1108:2011 “Ахборот технологияси. Очиқ тизимлар ўзаро боғлиқлиги. ЭРИ очиқ калити сертификати ва атрибут сертификатининг тузилмаси”;

3. O‘z DSt 1106:2009 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси”;

4. O‘z DSt ISO/IEC 9594-8:2018 “Ахборот технологияси. Очиқ тизимларнинг ўзаро боғлиқлиги. Очиқ калит ва атрибутлар сертификатининг структураси”.

5. O‘z DSt ISO/IEC 15945: 2015 “Ахборот технологияcи. Хавфсизликни таъминлаш усуллари. Электрон имзолар қўлланишини таъминлаш учун ИУТ хизматлари спецификацияси”.

“Электрон рақамли имзо тўғрисида” ги Ўзбекистон Республикаси Давлат солиқ қўмитаси ҳузуридаги рўйхатга олиш маркази томонидан берилган электрон рақамли имзо калити сертификатига эга бўлган шахслар давлат ва хўжалик бошқаруви органлари, маҳаллий давлат ҳокимияти органлари ҳамда тижорат банклари томонидан кўрсатиладиган барча турдаги хизматлардан эркин фойдалана олади.

Шу муносабат билан, Ўзбекистон Республикаси Давлат солиқ қўмитаси ҳузуридаги рўйхатга олиш маркази томонидан берилган ЭРИ калитлари “Электрон ҳукумат” тизимининг фойдаланувчини идентификациялашнинг ягона тизимида - id.gov.uz ва интерфаол давлат хизматларининг Ягона порталида - my.gov.uz сайтларида махсус модул ёрдамида фойдаланилмоқда.

Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги томонидан 2016 йил “Электрон рақамли имзо калитлари учун Рўйхатга олиш марказлари томонидан берилган электрон рақамли имзоларнинг ўзаро мувофиқлигини ва ҳақиқийлигини таъминлаш имкониятини таъминлаш талаблари” ишлаб чиқилган ва тасдиқланган.

Ушбу ҳужжатда электрон рақамли имзо очиқ калит сертификатининг таркиби, сақлаш форматига қўйиладиган талаблари тақдим этилган ва асосий маълумотларнинг узатилиши, электрон рақамли имзо калитлари форматининг универсаллигини амалга ошириш учун талаблар, электрон рақамли имзо калитлари форматини белгилайдиган объект идентификаторлари рўйхати кўрсатилган.

**II. Хорижий давлатлар электрон рақамли имзо тўғрисида қонунлари бўйича таҳлилий маълумот.**

**Хитой Халқ Республикаси**

**Қонун номи:** Хитой Халқ Республикасининг электрон имзо тўғрисидаги қонуни.

**Қонуннинг қисқача мазмуни:** Хитой қонуни Европа Иттифоқининг электрон имзолар тўғрисидаги директиваси, UNCITRAL намунавий қонунлари ва Бирлашган Миллатлар Ташкилотининг халқаро шартномаларда электрон алоқа тўғрисида конвенциялари асосида ишлаб чиқилган. Бу оддий электрон имзо ва электрон рақамли имзонинг мажбурий ижро этилишини таъминлайди. У икки даражали юрисдикция деб ҳисобланади, чунки у электрон рақамли имзоларга қўлда ёзилган имзо билан бир хил мақом беради, аммо оддий электрон имзоларни қонуний ва мажбурий деб тан олади. Ушбу моделга амал қилган мамлакатлар компанияларга имзоларнинг ҳар хил шаклларини танлаш ва ҳар бир фойдаланиш ҳолати учун энг қулай ва мос шакл асосида ўз бизнес жараёнларини созлаш имкониятини беради.

Электрон имзоларни аниқ ҳуқуқий қўллаб-қувватлашига қарамай, Хитойдаги баъзи судялар уларни тан олишга қарши бўлишмоқда. Натижада, меҳнат шартномалари каби нозик масалаларда қўлда ёзилган имзолардан фойдаланиш умкин.

**Асосий чекловлар**

Шахсий муносабатлар билан боғлиқ шартномалар (никоҳ, фарзандликка олиш, меросхўрлик каби), баъзи кўчмас мулк тўғрисидаги шартномалар ва коммунал хизматларни тўхтатиб қўйиш билан боғлиқ шартномалар қонундан озод қилинади.

**Европа Иттифоқи**

**Қонун номи:** Электрон идентификация ва ишончли хизматларни бошқариш тўғрисидаги низом (910/2014/EC).

**Қонуннинг қисқача мазмуни:** 1999 йилда Европа Иттифоқи электрон имзо тўғрисидаги йўриқномани (1999/93 / EC) қабул қилди. 2014 йил 23 июлда Европа Иттифоқи унинг ўрнига - Электрон идентификация ва ишончли хизматларни бошқариш тўғрисидаги низомни қабул қилди (910/2014/EC). Одатда eIDAS деб номланадиган ушбу меъёрий ҳужжат Европа Иттифоқи бўйлаб электрон идентификация қилиш, имзолар, муҳрлар ва ҳужжатлар учун янги ҳуқуқий тузилмани ўрнатади. eIDAS 2016 йил 1 июлдан кучга кирган. Шу санада Европа Иттифоқининг амалдаги кўрсатмаси, шунингдек Европа Иттифоқига аъзо давлатларнинг eIDASга зид бўлган барча қонунлари автоматик равишда бекор қилинади ёки ўзгартирилади. Биринчи марта, Европа Иттифоқининг барча ҳудудларида электрон имзо ва идентификаторларни тан олиш учун изчил қонунчилик базаси ва ягона бозор вужудга келди. Бу компанияларга Европа Иттифоқида электрон имзоларни ишлаб чиқиш ва улардан фойдаланишни кенгайтириш учун тахмин қилинадиган ҳуқуқий муҳитни тақдим этди.

eIDASнинг 25-моддасида барча электрон имзолар ва тасдиқлаш хизматлари суд ишларида далил сифатида қабул қилиниши мумкинлиги тўғрисидаги асосий ҳуқуқий қоидалар сақланиб қолган. Бунга электрон имзолар, муҳрлар, вақт штамплари, рўйхатдан ўтган етказиб бериш хизматлари ва веб-сайтни тасдиқлаш учун сертификатлар киради.

**Ҳиндистон Респупликаси**

**Қонун номи:** Ахборот технологиялари тўғрисидаги қонун.

**Қонуннинг қисқача мазмуни:** Ҳиндистон қонунларида оддий электрон имзо ҳам, рақамли имзо ҳам (баъзида кучайтирилган электрон имзо деб номланади) мажбурий ижро этилиши кўзда тутилган. У икки даражали юрисдикция деб ҳисобланади, чунки у рақамли имзоларга қўлда ёзилган имзо билан бир хил мақом беради, аммо оддий электрон имзоларни қонуний ва мажбурий деб тан олади. Ушбу моделга амал қилган мамлакатлар компанияларга имзоларнинг ҳар хил шаклларини танлаш ва ҳар бир фойдаланиш ҳолати учун энг қулай ва мос шакл асосида ўз бизнес жараёнларини созлаш имкониятини беради.

Ҳиндистонда электрон рақамли имзолардан фойдаланишда қўшимча техник ва қонуний талаблар мавжуд. Қонуннинг 35-моддасида, рақамли сертификатлар берадиган субъектлар учун стандартлар кўрсатилган.

**Асосий чекловлар**

Ишончномалар, васиятномалар ва кўчмас мулк билан боғлиқ шартномалар қонундан озод қилинган. Бундан ташқари, кўплаб битимларда штампланган қоғоздан фойдаланиш кераклиги тўғрисидаги талаб фарзандликка олишга халақит беради.

**Корея Республикаси**

**Қонун номи:** Рақамли имзо қонуни

**Қонуннинг қисқача мазмуни:** Корея Республикасининг Электрон имзо тўғрисидаги қонуни Европа Иттифоқининг электрон имзолар тўғрисидаги директиваси, UNCITRAL намунавий қонунлари асосида ишлаб чиқилган.

Бу оддий электрон имзо ва электрон рақамли имзонинг мажбурий ижро этилишини таъминлайди. У икки даражали юрисдикция деб ҳисобланади, чунки у электрон рақамли имзоларга қўлда ёзилган имзо билан бир хил мақом беради, аммо оддий электрон имзоларни қонуний ва мажбурий деб тан олади. Ушбу моделга амал қилган мамлакатлар компанияларга имзоларнинг ҳар хил шаклларини танлаш ва ҳар бир фойдаланиш ҳолати учун энг қулай ва мос шакл асосида ўз бизнес жараёнларини созлаш имкониятини беради.

Кўпгина бошқа мамлакатлар сингари, электрон имзоларга рухсат бериш учун ҳам розилик талаб қилинади. Аммо шартномани талқин қилишнинг умумий принтципига кўра, агар томонлар ўртасида бундай аниқ келишув мавжуд бўлмаса ёки имзолаган шахснинг кимлиги ёки юборилган хабарнинг ҳақиқийлиги ёки яхлитлиги шубҳа остига қўйилса, электрон имзонинг таъсирини томонларнинг ҳақиқий ниятини шарҳлаш йўли билан аниқлаш керак.

**Асосий чекловлар**

Хеч қандай муҳим чекловлар мавжуд эмас.

**Россия Федерацияси**

**Қонун номи:** Электрон имзо тўғрисида

**Қонуннинг қисқача мазмуни:** Россия қонунчилигига кўра имзонинг электрон эканлиги сабабли уни имзолашни рад этиш мумкин эмас. Бироқ, аниқ амалга оширилиши учун рақамли имзолар электрон ҳужжат алмашинувини таъминлаш учун ҳукумат томонидан сертификатланган, электрон курер вазифасини бажарадиган махсус хизмат кўрсатувчи провайдер орқали алмашиниши керак.

Шунингдек, қонунда электрон имзолар уч турга бўлинган:

* Оддий электрон имзо;
* Кучайтирилган электрон имзо (квалификацияланмаган);
* Кучайтирилган электрон имзо (квалификацияланган);

**Асосий чекловлар**

Хеч қандай муҳим чекловлар мавжуд эмас.

**Туркия Республикаси**

**Қонун номи:** ELEKTRONİK İMZA KANUNU

**Қонуннинг қисқача мазмуни:** Туркия UNCITRAL намунавий қонунига амал қилади ва кўплаб Европа Иттифоқига аъзо давлатларнинг қонунларига ўхшашдир. Бироқ, унинг қонунлари фақат рақамли, илғор ёки малакали электрон имзо деб аталадиган нарсаларнинг қонунийлигига қаратилган. Ушбу турдаги имзолар имзо чекувчи томон малакали хизмат кўрсатувчи провайдер томонидан берилган рақамли сертификатга эга бўлишини талаб қилади. Ушбу замонавий электрон имзолар қўлда ёзилган имзолар билан бир хил ҳуқуқий кучга эга. Туркия қонунчилигига биноан оддий электрон имзолар учун аниқ қоидалар мавжуд эмас.

**Асосий чекловлар**

Хеч қандай муҳим чекловлар мавжуд эмас.

**Америка қўшма штатлари**

**Қонун номи:** Глобал ва миллий тижорат тўғрисидаги қонунда электрон имзолар (ESIGN - Electronic Signatures in Global and National Commerce Act)

Ягона электрон оператсиялар тўғрисидаги қонун (UETA - Uniform Electronic Transactions Act)

**Қонуннинг қисқача мазмуни:** Федерал ҳукумат ESIGNни 2000 йилда қабул қилди. Бундан ташқари, ҳар бир штат электрон имзо тўғрисидаги қонунни қабул қилди, 47 таси UETA асосида версиясини қабул қилди. Ушбу минималист ёки рухсат берувчи қонунлар деярли барча турдаги шартномалар учун электрон имзолардан фойдаланишга рухсат беради. Шу билан бирга, бизнесни электрон шаклда олиб бориш учун барча томонларнинг олдиндан розилигини олиш муҳимдир.

**Асосий чекловлар**

ESIGN тўғрисидаги қонун ва аксарият штатлар қонунларида кўчмас мулкни топшириш, васиятномалар ва истеъмолчиларга қонуний равишда талаб қилинган баъзи хабарномалар бундан мустасно.

**III. Булутли электрон рақамли имзо тўғрисида.**

Булутли электрон имзо - бу ёпиқ, криптографик ҳимояланган ахборот ва ҳисоблаш тизими. Тизим шахсий калитларни яратиш ва электрон имзо сертификатини бериш, шунингдек Интернет тармоғи орқали электрон почта хабарларини тасдиқлаш имкониятини беради. Бу малакали имзонинг шахсий калитини булутда, Аккредитатсия қилинган ЭРИни хавфсиз ахборот тизимида сақлашни назарда тутади.

Булутда сақланган электрон имзо маҳаллий компютерда ўрнатилган рақамли имзо билан бир хил усулда фойдаланиши мумкин. Сиз ҳар қандай аҳамиятга эга бўлган ҳар қандай электрон ҳужжатларни тасдиқлашингиз мумкин. Шунингдек, булутли ЭРИ ички ва ташқи электрон ҳужжат айланиши тизимида ёки электрон савдо майдончаларида электрон савдо протцедураларида иштирок этиш учун ишлатилиши мумкин.

Булутли электрон имзолардан фойдаланишнинг асосий афзаллиги шундаки, охирги фойдаланувчи стационар иш жойига боғланишдан озод қилинади. Интернетга уланган қурилма мавжуд бӯлиши кифоя.

Европа давлатларида булутли ЭРИ ларни ишлатиш учун Европа телекоммуникация стандартлари институтининг ((European Telecommunications Standards Institute, ETSI)) Булутли стандартларини мувофиқлаштириш (Cloud Standard Coordination, CSC) гуруҳи талаблари асосида ишлатилади

Ахборот хавфсизлигини бошқариш тизимлари учун ISO 27001:2013 бўйича провайдерлар учун мажбурий сертификатлаш маълумотлар хавфсизлигини комплекс ҳимоя қилиш учун асосдир.

ISO 27017 стандартида ISO 27002 да мавжуд бўлмаган булут учун қўшимча хавфсизлик элементларини мавжуд. Ушбу стандартнинг тўлиқ расмий номи булутли хизматлар учун ISO/IEC 27002 қоидалари («Code of practice for information security controls based on ISO/IEC 27002 for cloud services») асосида ахборот хавфсизлигини бошқариш.

2014 йил ёзида ISO шахсий маълумотларни булутда ҳимоя қилиш бўйича ISO 27018 стандартини, 2015 йил охирида эса - булутли ечимлар учун ахборот хавфсизлигини бошқариш бўйича ISO 27017: 2015 стандартини нашр этди.

2014 йил кузида Европа парламентининг eIDAS деб номланган 910/2014-сонли янги регламенти кучга кирди. Янги қоидалар фойдаланувчиларга TSP (Trust Service Provider - Ишончли хизмат кўрсатувчи) деб номланган ишончли хизмат кўрсатувчи провайдернинг серверида сақлаш ва ундан фойдаланишга имкон беради.

Европа стандартлаштириш қўмитаси (CEN) 2013 йил октябр ойида булутли рақамли имзоларни тартибга солишга бағишланган "Сервер имзосини қўллаб-қувватлайдиган ишончли тизимлар учун хавфсизлик талаблари" CEN/TS 419241 «Security Requirements for Trustworthy Systems Supporting Server Signing» техник спетсификатсиясини қабул қилди. Ҳужжат хавфсизликка мувофиқликнинг бир неча даражасини тавсифлайди.